

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA**

IN THE MATTER OF THE SEARCH OF

Case No. : 3:19-mj-00241-DMS

7761 Mayfair Drive, Apt 3
Anchorage, AK

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

FILED UNDER SEAL

I, LISA WATSON, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND TASK FORCE OFFICER BACKGROUND

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been since 2010. In this assignment I have investigated a number of violations of United States Code. I am currently assigned to the Violent Crime Squad in the FBI Anchorage Field Office, and specifically assigned to work violent crimes against children investigations, including but not limited to internet crimes against children, online enticement of children, child pornography possession and distribution, and commercial sexual exploitation of children. I have also conducted investigations of human trafficking, civil rights violations, and public corruption. I have conducted and participated in numerous search warrants, arrest warrants, and interviews of people involved in various



JUN 13 2019

crimes. I have attended a number of conferences and trainings related to crimes against children and human trafficking investigations.

2. This affidavit is made in support of an application for a warrant to search 7761 Mayfair Drive, Apt 3, Anchorage, AK [hereinafter "SUBJECT RESIDENCE"], which is more particularly described in Attachment A, and to seize the items specified in Attachment B, which constitute instrumentalities, fruits, contraband, and evidence of violations, or attempted violations, of 18 U.S.C. § 1591, sex trafficking of minors, and 18 U.S.C. § 922(g)(1), prohibited person in possession of a firearm (felon in possession)

3. The statements in this affidavit are based in part on information provided to me by other law enforcement officers, police reports and on my own investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have only set forth the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1591 and 922(g)(1).

RELEVANT STATUTES

4. The following statutes are relevant to this affidavit:
- a. 18 U.S.C. § 1591 prohibits a person from knowingly in or affecting interstate or foreign commerce from recruiting, enticing, harboring, transporting, providing, obtaining, or maintaining by any means a person or

benefiting, financially or by receiving anything of value, from participation in a venture which has engaged in an act described above, knowing, or in reckless disregard of the fact, that means of force, threats of force, fraud, coercion, or any combination of such means will be used to cause the person to engage in a commercial sex act, or that the person has not attained the age of 18 years and will be caused to engage in a commercial sex act.

- b. 18 U.S.C. § 922(g)(1) prohibits a person who has been convicted in any court of a crime punishable by a term of imprisonment exceeding one year to ship or transport in interstate or foreign commerce, or to possess in an affecting interstate an foreign commerce, any firearm or ammunition, which has been shipped or transported in interstate or foreign commerce.

DEFINITIONS

5. The following terms are relevant to this affidavit in support of this application for a search warrant:

- a. *Commercial Sex Act:* The term commercial sex act means any sex act, on account of which anything of value is given to or received by any person. 18 U.S.C. § 1591(e)(3).
- b. *Coercion:* The term coercion means threats of serious harm to or physical restraint against any person, any scheme, plan, or pattern intended to cause a person to believe that failure to perform an act would result in serious

harm to or physical restraining against any person; or the abuse or threatened abuse of law or the legal process. 18 U.S.C. § 1591(e)(2).

- c. *Serious Harm*: The term serious harm means any harm, whether physical or nonphysical, including psychological, financial, or reputational harm, that is sufficiently serious, under all the surrounding circumstances, to compel a reasonable person of the same background and in the same circumstances to perform or to continue performing commercial sexual activity in order to avoid incurring that harm. 18 U.S.C. § 1591(e)(4).

6. The following technical terms are relevant to my affidavit in support of this application for a search warrant:

- a. As part of my training, I have become familiar with the Internet (also commonly known as the World Wide Web), which is a global network of computers¹ and other electronic devices that communicate with each other using various means, including standard telephone lines, high-speed telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions including cellular networks and satellite. Due to the structure

¹ The term "computer" is defined by 18 U.S.C. § 1030 (e) (1) to mean "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device."

of the Internet, connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via electronic mail (“e-mail”).

- b. Set forth below are an alphabetical listing of some definitions of technical terms, used throughout this Affidavit, and in Attachments A and B, hereto, pertaining to the Internet and computers more generally.

- i. Computer system and related peripherals, and computer media: As used in this Affidavit, the terms “computer system and related peripherals, and computer media” refer to tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drives and other computer-related operation equipment, digital cameras, scanners, in addition to computer photographs, and other visual depictions of



JUN 13 2019

such graphic interchange formats, including but not limited to, JPG, GIF, TIF, AVI, and MPEG.

- ii. Digital device: A “digital device” includes any electronic system or device capable of storing and/or processing data in digital form, including central processing units; desktop, laptop or notebook computers; tablets, internet-capable cellular phones (smart phones), or personal digital assistants; wireless communication devices such as telephone paging devices, beepers, and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices such as modems, cables, and connections; storage media such as hard disk drives, flash drives, thumb drives, floppy disks, compact disks, DVDs, magnetic tapes, and memory chips; and security devices.
- iii. Image or copy: An “image or copy” is an accurate reproduction of information contained on an original physical item, independent of the electronic storage device. “Imaging” or “copying” maintains contents, but attributes may change during the reproduction.
- iv. Log files: “Log files” are records automatically produced by computer programs to document electronic events that occur on


JUN 13 2019

computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a web site was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

- c. The terms “*records*” and “*information*” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writings, drawings or paintings); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

//

//

//

//

//


JUN 13 2019

FACTS IN SUPPORT OF PROBABLE CAUSE

Background on Pimp Culture and the Use of Cellular Phones

7. Through my training and experience, I am aware of the following traits of prostitution, and how the Internet and cell phones are used to further the activities of illegal prostitution:

- a. Individuals who, through enticement, intimidation, or force, enlist individuals to become prostitutes, and who profit from the prostitution of others are called "pimps." Pimps are sometimes euphemistically referred to as "management."
- b. Pimps, as well as prostitutes who are not "managed," have embraced the internet as a means of advertising services and communicating with customers.
- c. Certain web sites have been created to facilitate communications between prostitutes and their clients. These web sites allow pictures to be posted as part of advertisements. I have viewed prostitution advertisements on these web sites, including on skipthegames.com
- d. Subjects who utilize the internet to post prostitution related advertisements on websites often use photographs in the advertisements. These photographs often show a nude or semi-nude female. Sometimes these females are under the age of 18 years old.


JUN 13 2019

- e. Advertisements for prostitutes often contain codes for the services provided. For example the term "w4m" means women for men. The term "in-calls only" refer that the prostitute will be providing the location for the sexual transaction. An "outcall" means that the prostitute will travel to the customer's location. The term "donation" is often used to mean the cost for the sexual transaction. In some instances, code words are used to indicate the cost of the transaction. For instance, a reference to a "donation of 100 roses" would mean that the sexual act costs \$100.
- f. Pimps attempt to avoid the attention of law enforcement through the anonymity provided by the Internet.
- g. Most juvenile prostitutes have pimps. Prostitutes will often refuse to divulge the identity of their pimps to law enforcement. Most pimps often instruct their prostitutes on what to say and what not to say to law enforcement.
- h. Prostitutes are instructed by the pimp on how to detect undercover officers. When arranging "dates" with clients over the phone, prostitutes rarely discuss the details pertaining to the sexual acts that are to occur until they meet in person.
- i. Pimps sometimes use physical force and/or fear to control their prostitutes. They control the prostitutes' actions and collect monies earned through acts


JUN 13 2019

of prostitution. Pimps facilitate the prostitution by transporting the prostitutes to locations where the prostitution occurs. Pimps sometimes transport prostitutes across state lines for the purpose of prostitution.

- j. Prostitutes and/or pimps often stay in motels/hotels while traveling. Prostitutes and pimps travel via rental vehicles, vehicles, airplane, or bus during their travels. The pimps utilize the monies earned during acts of prostitution to purchase food, lodging, clothing and other items.
- k. Pimps often possess firearms to assist in protecting and intimidating their prostitutes.
- l. Some pimps sell drugs as another means to make money. Pimps sometimes provide drugs to the prostitutes to suppress their appetites and to assist with the demands of prostituting for long periods of time.
- m. Pimps can be either male or female.
- n. The term "daddy" is commonly used by prostitutes when referring to their pimps. The pimp's phone number is often programmed as "daddy" in the prostitute's cell phone.
- o. Pimps often request or force their prostitutes to obtain tattoos of names and/or symbols that are related to the pimp's name or nickname.
- p. Prostitutes utilize cellular telephones as a way to be contacted by clients.


These phone numbers are included in the advertisements that are posted on

various prostitution assisting web sites. Contact is made through phone calls as well as text messages and social media.

- q. Pimps and their prostitutes communicate with each other through cellular phones regarding prostitution activity. Communication is made through phone calls as well as text messages.
- r. Pimps and prostitutes communicate with others involved in the prostitution/pimp sub-culture either by phone calls, text messages, and social media regarding prostitution/pimp activities.
- s. Pimps and their prostitutes use cellular telephone cameras to take photographs of the prostitutes used in the prostitution advertisements.
- t. Pimps and their prostitutes use cellular telephones to transmit photographs to email accounts, social media accounts, and/or prostitution assisted internet sites.
- u. Pimps and prostitutes use personal e-mail accounts to post their advertisements on prostitution assisting web sites.
- v. It is common for individuals to carry cell phones, smart phones, tablets, and other similar devices on their person.

Identification of Minor Victim 1 and Jayshon Moore a/k/a "China"

8. The FBI first became aware of Minor Victim 1 in October 2017 as a possible victim of sex trafficking. Minor Victim 1 was fifteen years old at that time. The


JUN 13 2019

FBI was contacted by Office of Children Services and Whaley School regarding their concerns. Agents met with Minor Victim 1 and she reported she had been physically assaulted. She had bruises and reported neck pain and difficulty seeing out of one eye. Agents transported her to the hospital. At that time, Minor Victim 1 stated she was assaulted by "A" but would not provide any further details about the perpetrator or her situation.

9. On December 26, 2018, the FBI interviewed Minor Victim 1 regarding a different sex trafficking case relating to Tristan Grant. In that interview, Minor Victim 1 said that she worked for Grant along with two other minors. The FBI interviewed one of these minors (hereinafter "Minor Witness A") on January 3, 2019. She stated she knew Minor Victim 1 and that Minor Victim 1 was living with a pimp named "China." Minor Witness A thought "China's" real name was Jayshon, and he was about thirty-five years old. Minor Witness A also stated "China" tried to pimp her out but did not provide any further information.

10. In a post-*Miranda* interview of Grant on December 12, 2018, Grant stated he knew Minor Victim 1 and that she was being prostituted by "China," whom he described as Minor Victim 1's husband/pimp. Grant also stated that Minor Victim 1's sister was also involved in the sex trafficking of Minor Victim 1. Grant is currently indicted for production of child pornography involving a Minor Witness A, and for being a felon in possession of firearms. Grant is also suspected of prostituting a third minor.

11. In interviews on December 17, 2018 and January 25, 2019 with Ajela Banks, Banks stated that Minor Victim 1 was working for a pimp named "China," that he "turned out" (got her started in prostitution), and got her addicted to drugs. Banks is currently indicted for production and possession of child pornography. She is also suspected of conspiring with Grant on the prostitution of Minor Victim 1, Minor Witness A, and a third minor.

12. On January 2, 2019, Minor Victim 1's older sister was interviewed. She stated Minor Victim 1 was currently in a romantic relationship with Jayshon. Minor Victim 1's sister said that Jayshon is also known as "China."

13. On June 7, 2019, APD was called to the SUBJECT RESIDENCE after receiving a report of a female screaming. Upon arriving at the SUBJECT RESIDENCE, Jayshon Moore told officers that his girlfriend, Minor Victim 1, was upset with him, threw items, and broke a table. Minor Victim 1 admitted she caused the damage. Minor Victim 1 told officers she had been dating Moore for two years but didn't move into his residence until three months ago. Minor Victim 1 called Moore "a baby killer," and said he made her get an abortion. Minor Victim 1 told officers Moore pushed her into a dog kennel, injuring her head and also pushed her down the stairs outside the apartment. Law enforcement did not observe any injuries on Minor Victim 1 consistent with these allegations. Minor Victim 1 was arrested and during transport to McLaughlin Youth


JUN 13 2019

Center (MYC) bit one of the officers in the hand. Minor Victim 1 was charged with DV Criminal Mischief 5, Resisting Arrest, and Assault.


Interview of Minor Victim 1 on June 11, 2019

14. On June 11, 2019, FBI Task Force Officer Torres interviewed Minor Victim 1 at MYC. During this interview, Minor Victim 1, provided the following information:

- a. Minor Victim 1 stated she has been with Moore for three years. She met him through her older sister. Minor Victim 1 was 14 years old when she first met Moore. Minor Victim 1 initially told Moore she was 18 years old but Moore learned her true age when she was 15 years old.
- b. Minor Victim 1 stated on the day of her arrest, Moore woke her up trying to give her some “clear.”² She got up and saw her cigarettes were gone and got angry with Moore. Minor Victim 1 stated Moore was angry with her because she would not put her high-heeled shoes on and walk Spenard.³ Minor Victim 1 stated Moore makes her walk up and down Spenard as punishment if she does something bad.

² “Clear” is a common street name for methamphetamine.

³ Spenard is a common “track” in Anchorage where law enforcement knows individuals walk in order to meet customers for the purpose of engaging in commercial sex transactions.


JUN 13 2019

- c. Minor Victim 1 stated she does not have a quota of money or dates but has to make money to give to Moore to pay the rent. She stated she has three weeks to make approximately \$1,000. Minor Victim 1 stated if she does not get enough dates online she has to walk Spenard as punishment.
- d. Minor Victim 1 has posted on www.skipthegames.com⁴ for dates. She does in-calls – commercial sex acts where the customer comes to the location of the prostitute - at the SUBJECT RESIDENCE. Moore also described doing car dates in which the commercial sex acts were performed in a customer's automobile. Minor Victim 1 set up her profile on "skipthegames" and posted because Moore was unfamiliar with how to do that. She said she posted under the name "Coffee."
- e. Minor Victim 1 initially stated she started working for Moore as a prostitute three months before her arrest, but later stated it was a year prior, when she was 15 years old. Moore drove Minor Victim 1 to Spenard to walk and do car dates. Moore found dates for her and charged \$140 for half hour and \$250 for an hour. Sex acts such as oral sex and handjobs were \$80 to \$100. Customers who paid \$200 or \$250 could get whatever sex act they wanted.

⁴ Skipthegames.com is known to law enforcement as a common online marketplace for prostitutes to advertise for customers.


JUN 13 2019

Minor Victim 1 used condoms during sex with customers. Minor Victim 1 gave all of the money from her dates to Moore.

- f. Minor Victim 1 stated she wasn't being completely honest about her history with Moore because she loved him. Minor Victim 1 stated she did ten dates for Moore and all of the other dates were on her own. She also stated she did prostitution dates for him in the past but recently stopped because she didn't want to do dates anymore and only wanted to be with Moore.
- g. Minor Victim 1 stated Moore has had other females working for him. At one point she was living at her Dad's house and Moore told her the only way she could come back to him was if she "ho'd" for him.
- h. Minor Victim 1 also stated Moore deals drugs such as methamphetamine and crack cocaine. Minor Victim 1 stated that she has done drug runs for Moore, meaning she has traveled for him and brought drugs back to Alaska on her return trip, and that she has sold cocaine and meth for him.
- i. Moore gave Minor Victim 1 methamphetamine to get her up and energized for dates. If she didn't get up, he would make her put high heels on and walk Spenard with no drugs in her system. Minor Victim 1 also stated Moore has physically assaulted her.
- j. Minor Victim 1 said Moore has guns in his home and in the storage outside at his house. Minor Victim 1 said he had other guns around his house. She

stated she has hid guns for him around the house. On one occasions when police came to the SUBJECT RESIDENCE, she hid a gun under the mattress. She stated that Moore has both handguns and rifles.

k. Minor Victim 1 stated Moore is on the lease at the apartment (SUBJECT RESIDENCE).

l. Minor Victim 1 has a Motorola cell phone, which was left with Moore at SUBJECT RESIDENCE upon her arrest on June 7, 2019.

Jayshon Moore

15. In 2010, Jayshon Moore was convicted in the United States District Court in Anchorage of Felon in Possession and Drug Distribution. He was sentenced to 87 months incarceration and 36 months supervised release. Moore is currently on supervised release with United States Probation.

16. A review of the Alaska Public Safety Information Network revealed that on April 17, 2019, Jayshon Moore listed his mailing and residential address as 7761 Mayfair Drive #3, Anchorage, Alaska.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

17. Searches and seizures of evidence from computers and other Internet access devices require agents to seize most or all electronic items (hardware, software, passwords and instructions) to be processed later by appropriate personnel in a controlled environment. Digital storage media may include but is not limited to floppy disks, hard

drives, tapes, DVD disks, CD-ROM disks or other magnetic, optical or mechanical storage which can be accessed by computers or other electronic devices to store or retrieve data, which can store the equivalent of thousands of pages of information. Users may store information or images in random order with deceptive file names, which requires searching authorities to examine all the stored data to determine whether it is included in the search warrant. This sorting process renders it impractical to attempt this kind of data search on site.

18. Searching digital evidence systems for criminal evidence requires experience in the computer and cellular telephone field and a properly controlled environment in order to protect the integrity of the evidence and recover even “hidden,” erased, compressed, password-protected, or encrypted files. Since digital evidence is extremely vulnerable to tampering or destruction (both from external sources and from destructive code imbedded in the system as a “booby trap”), a controlled environment is essential to its complete and accurate analysis.

19. Computers and other digital communications devices contain volatile memory that contains information only while the device is in a powered on and/or running state. I know that powering off the device may result in the loss of the volatile information. Adding an external evidence storage device will cause minor changes to the state of the computer but will allow for the best effort in fully capturing the state of the running evidence. This capture of information requires technical expertise to ensure the


JUN 13 2019

resulting data can be examined by all subsequent investigators. This captured information may include current and recent use of the computer, use of encryption, use of other communications devices, routes of Internet and other digital communications traffic and passwords, encryption keys or other dynamic details relevant to use of the system.

20. In order to fully retrieve data from a computer or other digital communications system, the analyst needs all magnetic storage media as well as the storage devices. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware access software or drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) as well as all instruction manuals or other documentation and data security devices, and all items containing or displaying passwords, access codes, usernames or other identifiers necessary to examine or operate items, software or information seized or to activate specific equipment or software. In cases like the instant one where the evidence consists partly of image and video files, the monitor and printer are essential to show the nature and quality of the graphic images, which the system could produce. Finally, where there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, and modem, hardware and software are all instrumentalities of the crime of possession, receipt, or transportation of sexually explicit depictions of minors in violation of federal law, they should also all be seized as such.

21. As further described in Attachment B, this warrant seeks permission to locate in the SUBJECT RESIDENCE not only computer files that might serve as direct evidence of the crimes described in the warrant, but also for evidence that establishes how computers were used, the purpose of their use, and who used them. Further, as described above and in Attachment B, this application seeks permission to search and seize records that might be found in the SUBJECT RESIDENCE, in whatever form they are found. One form in which the records might be found is that they are stored on a computer's hard drive, or other electronic media. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis of the computer(s) or other electronic storage media seized.

22. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processor, picture, and movie files), computer hard drives can contain other forms of electronic evidence as well. In particular, records of how a computer has been used, the purposes for which it was used, and who has used it are called for by this warrant. As described above, data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the hard drive that show what tasks

and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs store configuration information on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals (e.g., cameras and printers for creating or reproducing images), the attachment of USB flash storage devices, and the times and dates the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created. This information can sometimes be evidence of a crime, or can point toward the existence of evidence in other locations. Evidence of this type is a conclusion, based on a review of all available facts and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand the evidence described in Attachment B is included within the scope of the warrant.

23. In finding evidence of how a computer has been used, the purposes for which it was used, and who has used it, sometimes it is necessary to establish that a particular thing is not present on a drive. For example, I know from training and experience that it is possible that malicious software can be installed on a computer, often without the computer user's knowledge. This software can allow a computer to be used by others. To investigate the crimes described in this warrant, it might be necessary to investigate whether any such malicious software is present on the computer, and, if so,

whether the presence of that malicious software might explain the presence of other things found on the computer's hard drive.

24. Law enforcement personnel trained in searching and seizing computer data will seize items of evidentiary value, and transport the same to an appropriate law enforcement laboratory for off-site review. The electronic media will be reviewed for the evidence described in Attachment B in accordance with and as defined by the review protocols described below.

25. I am familiar with and understand the implications of the Privacy Protection Act (PPA), 42 U.S.C. § 2000aa, and the role of this statute in protecting First Amendment activities. I am not aware that any of the materials to be searched and seized from the SUBJECT RESIDENCE are protected materials pursuant to the PPA. If any such protected materials are inadvertently seized, all efforts will be made to return these materials to their authors as quickly as possible.

26. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard


JUN 13 2019

drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - for long periods of time before they are overwritten. Files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. The search for these files and file fragments can take considerable time, depending on the computer user's practices.

27. I know from training and experience that computers or other digital devices used to access the Internet usually contain files, logs or file remnants which would tend to show ownership and use of the device, ownership and use of any external devices that had been attached to the computer or other digital devices, as well as ownership and use of Internet service accounts used for the Internet or cellular data network access.

28. I know from training and experience that digital crime scenes usually include items or digital information that would tend to establish ownership or use of


JUN 13 2019

digital devices and Internet access equipment and ownership or use of any Internet service or digital cellular service accounts used in this case.


SPECIFIC METHODS OF SEARCHING FOR DIGITAL EVIDENCE

Authority to Search Residents and Guests of the SUBJECT RESIDENCE

29. Because some of the items described in Attachment B may be carried on a person, for instance, cell phones and other digital devices, weapons, or drugs used, this warrant seeks authority to search the person of any residents or long-term guests of the SUBJECT RESIDENCE, who are found at the property, and who might possess items sought in the search warrant, and to seize from those individuals any evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1591 and 922(g)(1).

Seizure of Digital Evidence

30. I am seeking authority to search for, among other things, items containing digital data, more particularly described in Attachment B. This is so because there is evidence in this case that a Motorola cell phone has been used to post prostitution advertisements relating to a minor. In addition, Minor Victim 1 and Banks have provided information about Moore providing drugs to Minor Victim 1, in part as a means to control the activities of Minor Victim 1 and induce and coerce her to work as a prostitute for him. Furthermore, in my training and experience, a cell phone or other internet-capable device is frequently used by drug purchasers to coordinate the purchase of controlled substances. In addition, in my training and experience, cell phones and other


JUN 13 2019

modern internet-capable devices are essential components of sex trafficking. For instance, as detailed above, cell phones are used by pimps for numerous purposes, including to communicate with individuals who work for them, and to communicate with customers.

31. I also know in my training and experience that one method used by prohibited persons to purchase illegal firearms is through online sales. This is so because sales coordinated through online marketplaces do not require the completion of government paperwork associated with the sale of weapons through licensed gun dealers operating brick and mortar business, or the use of straw purchasers. Identification of weapons for sale online, and communication with the sellers of those weapons frequently takes place by text messaging or email through a cell phone or other internet-capable device.

32. Consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

33. The search of a computer hard drive or other computer storage medium is a time-consuming manual process often requiring months of work. This is so for a number of reasons, including the complexity of computer systems, the multiple devices upon which computing can take place, and the tremendous storage capacity of modern day computers, and the use of encryption or wiping software. As explained above, modern day computers and storage devices are capable of holding massive quantities of data, and the volume of evidence seized in these cases can be immense. I know from my training and experience, and from my discussions with trained computer forensic examiners, that a review of such quantities of evidence can take a significant amount of time. Second, there is a limited pool of personnel capable of conducting a forensic examination. Third, in some instances an individual may utilize encryption software or other publically-available techniques such as wiping software to hide data. Forensic tools are available to circumvent some of these techniques; however, these tools may require a significant allocation of resources and a substantial period of time.

34. Some or all of the following search methods may be used to conduct the forensic search in this case. These methods are not listed in any particular order, nor is their listing in this affidavit a representation that they will be used in this or any other case. Moreover, this list is simply provides an example of techniques that may be used, and is not intended to bind the forensic examiner to only these techniques:


JUN 13 2019

- a. *Keyword Searches*: I know that computer forensic utilities provide the capability for a user to search for specific key words that may exist on a piece of digital media. I intend to use specific keywords known to be related to either the subject's illicit internet activities. Those keyword searches will indicate files and other areas of the hard drive that need to be further reviewed to determine if those areas contain relevant data. A list of keywords utilized will be maintained with the records of the forensic examination.
- b. *Data Carving*: I know that, as previously mentioned, data residue may be left in the "free," "unallocated," or "slack" space of a computer hard drive, that is, the space not currently used by active files. I further know that, as previously mentioned, many operating systems utilize temporary storage often referred to as "swap space" on the hard drive to store contents from main system memory. Such unallocated and swap space may contain the residue of files that can be carved out, often in an automated or semi-automated fashion. I intend to use forensic tools to carve out files, in particular, image files such as JPEG and GIF files. The mere act of carving out such files does not expose me to the contents of such recovered files, but makes those files available for further relevancy checks, such as



JUN 13 2019

keyword searches (explained above) and hash value comparisons (explained below).

- c. *File Header / Extension Checks*: I know that individuals involved in illegal activities on a computer often change the extension of a file (such as .jpg) to some other incompatible extension (such as .txt) in order to disguise files from casual observers. The extension of a file, however, is not necessarily linked to the "header" of a file, which is a unique marking imbedded automatically in many types of files. By comparing the extension of a file with the "header information" of a file, it is possible to detect attempts to disguise evidence of illegal activities. Such a comparison can be made in an automated process by computer forensic tools. I intend to run an automated header comparison to detect such efforts, and intend to review any such files that reasonably may contain the evidence sought in this warrant.
- d. *Thumbnail / Image Views*: Although hash value comparisons can positively identify images, a negative hash value comparison does not exclude an image from suspicion. There is no known alternative for visually inspecting each image file. I therefore intend to examine at least a thumbnail image of each image file on the digital media whether "live," "data carved," or identified by header.


JUN 13 2019

- e. *Registry / Log File Checks*: I know that it is necessary in any criminal case to establish not only that a crime has occurred, but also to establish what person committed that crime. Operating systems and computer programs often maintain various administrative files such as logs that contain information about user activities at certain times. In the Windows operating system, for example, some of these files are collectively referred to as "the registry". Such files contain specific information about users, often including e-mail addresses used, passwords stored, and programs executed by a particular user. These files may also contain evidence regarding storage devices that have been connected to a computer at some time. Multiple backup copies of such files may exist on a single computer. I intend to examine these files to attempt to identify the evidence sought in this warrant, and to establish methods (such as software used) and dates of this activity.
- f. *Metadata / Alternative Data Streams*: I know that many file types, operating systems, and file systems have mechanisms for storing information that is not immediately visible to the end user without some effort. Metadata, for example, is data contained in a file that is not usually associated with the content of a file, but is often associated with the properties of the application or device that created that file. For example,



JUN 13 2019

digital camera photograph often has hidden data that contains information identifying the camera that manufactured it, and the date the image was taken. Some file systems for computers also permit the storage of alternate data streams, whereby a file such as a text file may hide an image file that would not be immediately visible to an end user without some action taken. Metadata and alternative data streams are often identified and processed automatically by computer forensic utilities. I intend to review any such data that is flagged by any process above as being relevant to the evidence sought in this warrant.

35. With rare exception, the above-listed search techniques will not be performed on original digital evidence. Instead, I know that the first priority of a digital evidence forensic examination is the preservation of all data seized. As such, original digital media will be, wherever possible, copied, or "imaged," prior to the start of any search for evidence. The copy will be authenticated digitally as described in the paragraph below.

36. I know that a digital forensic image is the best possible copy that can be obtained for a piece of digital media. Forensic imaging tools make an exact copy of every accessible piece of data on the original digital media. In general, the data contained on the original media is run through a hashing algorithm as described above, and a hash value for the entire device is generated. Upon completion of the imaging



JUN 13 2019

process, the same hash algorithm is run on the imaged copy to insure the copy is an exact duplicate of the original.

37. Criminal Procedure Rule 41 specifically states “The officer may retain a copy of the electronically stored information that was seized or copied.” Fed. R. Crim. P. 41 (f)(1)(B). Moreover, upon identification of contraband, the item is subject to forfeiture, and the owner has a reduced expectation of privacy in those seized devices. Consequently, should a seized device be found during the authorized forensic review to contain contraband, it will be retained by the United States, and may be searched without further authorization of the Court for the evidence described in Attachment B. Such a later search may be required for the following reasons:

- a. Should the execution of the warrant uncover data that may later need to be introduced into evidence during a trial or other proceeding, the authenticity and the integrity of the evidence and the government's forensic methodology may be contested issues. Retaining copies of seized storage media may be required to prove these facts.
- b. Returning the original storage medium to its owner will not allow for the preservation of that evidence. Even routine use may forever change the data it contains, alter system access times, or eliminate data stored on it.
- c. Because the investigation is not yet complete, it is not possible to predict all possible defendants against whom evidence found on the storage medium



JUN 13 2019

might be used. That evidence might be used against persons who have no possessory interest in the storage media, or against persons yet unknown.

Those defendants might be entitled to a copy of the complete storage media in discovery. Retention of a complete image assures that it will be available to all parties, including those known now and those later identified.

- d. The act of destroying or returning storage medium could create an opportunity for a defendant to claim, falsely, that the destroyed or returned storage medium contained evidence favorable to him. Maintaining a copy of the storage medium would permit the government, through an additional warrant if necessary, to investigate such a claim.
- e. Similarly, should a defendant suggest an explanation for the presence of evidence on storage medium or some defense, it may be necessary to investigate such an explanation or defense by, among other things, re-examining the storage medium with that explanation or defense in mind. This may require an additional examination of the storage medium for evidence that is described in Attachment B but was not properly identified and segregated previously.



JUN 13 2019

38. In the event that a piece of digital media is found not to be (a) an instrumentality of the offense, (b) a fruit of the criminal activity, (c) contraband, or (d) evidence of the offenses specified herein, it will be returned as quickly as possible.

39. As it concerns computer evidence, this warrant does not contain a limitation on the locations within a digital device that may be searched, or the types of data that may be seized from those locations. This is so for multiple reasons, each of which has been addressed in greater detail above. First, sophisticated computer users are able to manipulate the data on their computers to hide contraband or alter information associated with a contraband file. Without the ability to examine all parts of the computer, and all files located therein, it is impossible to know for certain whether or not contraband is present. Second, individuals may use multiple platforms within their digital devices to acquire images, such as open searches on the Internet (i.e. Google), Internet-based file-sharing services, and other third-party applications (“Apps”). Therefore, it is necessary in any search of a digital device to be able to examine the entirety of the computer without limitation to date ranges, programs, or file types, in order to be able to ensure that each of these platforms have been examined.

REQUEST FOR SEALING

40. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application. I believe that sealing this document is necessary because the full scope of this investigation is not



JUN 13 2019

yet public, and disclosure of the facts and statements contained in this affidavit may have a significant and negative impact on this case. Specifically, the United States is aware of the history of violence perpetrated by multiple subjects named in this search warrant, and suspects that threats to witnesses may be made should the full extent of the investigation be published at this time. The result is that if the search warrant is publicly filed, the subject of this investigation, and others associated with him, to include possible coconspirators, may flee or take steps to conceal or tamper with evidence which could seriously jeopardize the investigation.

CONCLUSION

41. Based upon the information above, your affiant submits that there is probable cause to believe that violations of 18 U.S.C. §§ 1591 and 922(g)(1) have been committed, that the items described in Attachment B are evidence, fruits, and instrumentalities of those violations and that the items described in Attachment B are likely to be found at the premises described in Attachment A.

//

//

//

//

//

//


JUN 13 2019

42. I request that the Court issue a warrant authorizing a search of the
SUBJECT PREMISES that is described in Attachment A, for the items described in
Attachment B.

Lisa Watson

LISA WATSON
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me this
13 day of June 2019

Deborah M. Smith

DEBORAH M. SMITH
Chief United States Magistrate Judge
District of Alaska
Anchorage, Alaska



JS

JUN 13 2019